I

111TH CONGRESS
1ST SESSION

H. R. 2195

To amend the Federal Power Act to provide additional authorities to a
quately protect the critical electric infrastructure against cyber
and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 30, 2009

Mr. THOMPSON of Mississippi (for himself, Mr. KING of New York, Ms.
CLARKE, Mr. DANIEL E. LUNGREN of California, Ms. JACKSON-LEE of
Texas, Ms. LORETTA SANCHEZ of California, Ms. HARMAN, Mr.
CUELLAR, Mr. CARNEY, Ms. ZOE LOFGREN of California, Mr. PASCRELL,
Mr. LUJÁN, and Mr. LANGEVIN) introduced the following bill; which was
referred to the Committee on Energy and Commerce, and in addition to
the Committee on Homeland Security, for a period to be subsequently d
termined by the Speaker, in each case for consideration of such provi
as fall within the jurisdiction of the committee concerned

A BILL

To amend the Federal Power Act to provide additional au
thorities to adequately protect the critical electric
structure against cyber attack, and for other purpos

Be it enacted by the Senate and House of Represent
tives of the United States of America in Congress asse

SECTION 1. CRITICAL ELECTRIC INFRASTRUCTURE.

(a) FINDINGS.—

(1) The critical electric infrastructure of t
United States and Canada has more than $1 trillion

in asset value, more than 200,000 miles of trans
mission lines, and more than 800,000 megawatts of
generating capability, serving over 300 million pe
ple.

(2) The effective functioning of this infrastru
ture is highly dependent on computer-based control
systems that are used to monitor and manage sen-
sitive processes and physical functions.

(3) These control systems are becoming increas-
ingly connected to open networks, such as corporat
intranets and the Internet. According to the Depart
ment of Homeland Security's United States Com-
puter Emergency Readiness Team (''US–CERT''),
this transition towards widely used technologies a
open connectivity exposes control systems to the
ever-present cyber risks that exist in the informat
technology world in addition to control system spe
cific risks.

(4) Malicious actors pose a significant risk t
this infrastructure. The Federal Bureau of Inves-
tigation (''FBI'') has identified multiple sources
threats, including foreign nation states, domest
criminals and hackers, and disgruntled employees.

(5) Intentional or naturally occurring Electro
magnetic Pulse (''EMP'') events also threaten crit

ical electric infrastructure. The Commission to As
sess the Threat to the United States from EMP At-
tack reported in 2008 that an EMP attack could
cause significant damage or disruption to critic
electric infrastructure and other critical infrast
ture due to the widespread use of Supervisory Con-
trol and Data Acquisition (''SCADA'') systems. The
National Academy of Sciences also reported in 2008
that Severe Space Weather Events could produce
similar results.

(6) The Department of Homeland Security's Control Systems Security Program is designed to in-
crease the reliability, security, and resilience o
trol systems to guard against and enhance domestic
preparedness for and collective response to a cyb
attack by a terrorist or other person. This is do
by developing voluntary cyber risk reduction prod
ucts, supporting the Department of Homeland Secu-
rity's Industrial Control Systems Computer Emer-
gency Response Team (''ICS-CERT'') in developing
vulnerability mitigation recommendations and strate
gies, and coordinating and leveraging activities
improving the Nation's critical infrastructure sec
rity posture.

(7) According to recent news reports, the elec
tronic control systems of the electrical system in
United States have been routinely penetrated and
compromised. According to current and former na-
tional security officials, cyber spies from China,
sia, and other countries have penetrated the Unite
States electrical system in order to map the syste
and have left behind software programs that could
be used to disrupt and disable the system.

(8) In the interest of national security, and
enhance domestic preparedness for and collective re
sponse to a cyber attack by a terrorist or other p
son, a statutory mechanism is necessary to protec
the critical electric infrastructure against cy
threats.

(9) In spite of existing mandatory cybersecurity
standards, a report from the North American Elec-
tric Reliability Corporation (''NERC'') suggests th
many utilities are underreporting their assets, pot
tially to avoid compliance requirements. In Apri
2009, NERC reported that only 23 percent of re-
sponding utilities identified a ''Critical Cyber As
as required by NERC Reliability Standard 002–1.
According to NERC, the results of this survey sug-
gest that utilities may not have identified cert

qualifying assets as ''Critical''. NERC requeste that entities take a fresh, comprehensive look a their methodology in order to identify and secur more Critical Cyber Assets.

(10) On May 21, 2008, in testimony before the House Committee on Homeland Security, Joseph Kelliher, then-Chairman of the Federal Energy Reg- ulatory Commission (''the Commission''), stated tha his agency is in need of additional legal authori to adequately protect the electric power system against cyber attack.

(b) RESEARCH ON CYBER COMPROMISE OF CRITICAL ELECTRIC INFRASTRUCTURE.—(1) Pursuant to section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) and in furtherance of domestic preparedness for and co lective response to a cyber attack by a terrorist or person, the Secretary of Homeland Security, working wit other national security and intelligence agencies, shal duct research and determine if the security of feder owned programmable electronic devices and communica- tion networks (including hardware, software, and data) sential to the reliable operation of critical electri structure have been compromised.

(2) The scope of the research referred to in para graph (1) shall include: the extent of compromise, ide

fication of attackers, the method of penetration, rami
tions of the compromise on future operations of crit
electric infrastructure, secondary ramifications of the
promise on other critical infrastructure sectors and
functioning of civil society, ramifications of compro
on national security, including war fighting capability
recommended mitigation activities.

(3) The Secretary of Homeland Security shall report the findings to the appropriate committees of Congres including the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate. The report may contain a classified annex.

(c) FEDERAL POWER ACT AMENDMENT.—Part II of the Federal Power Act (16 U.S.C. 791a and following) is amended by adding the following new sections at t end thereof:

"SEC. 224 CRITICAL INFRASTRUCTURE.

''(a) DEFINITIONS.—For purposes of this section:

''(1) CRITICAL ELECTRIC INFRASTRUCTURE.—

The term 'critical electric infrastructure' means s tems and assets, whether physical or cyber used fo the generation, transmission, distribution, or mete ing of electric energy that, in the determination the Commission, in consultation with the Secretary

of Homeland Security and other national security agencies, are so vital to the United States that incapacity or destruction of such systems and asset either alone or in combination with the failure other assets, would cause significant harm to the s curity, national or regional economic security, or tional or regional public health or safety.

''(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure inf mation related to critical electric infrastructure.

''(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the same meaning as is given that term in sec tion 212(3) of the Critical Infrastructure Informa tion Act of 2002 (6 U.S.C. 131(3)).

''(4) CYBER THREAT.—The term 'cyber threat' means any act by a terrorist or other person tha disrupts, attempts to disrupt, or poses a signific risk of disruption to the operation of programmabl electronic devices and communication networks (in- cluding hardware, software, and data) essential t the reliable operation of critical electric infra ture.

''(5) CYBER VULNERABILITY.—The term 'cyber vulnerability' means any weakness that, if exploit by a terrorist or other person, poses a signific risk of disruption to the operation of programmabl electronic devices and communication networks (in- cluding hardware, software, and data) essential t the reliable operation of critical electric infra ture.

''(b) ASSESSMENT, REPORT, AND DETERMINATION.—

''(1) IN GENERAL.—Pursuant to section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121), the Secretary of Homeland Security shall assess cyber vulnerabilities or threats to critical infra ture, including critical electric infrastructure an vanced metering infrastructure, on an ongoing basi and produce reports, including recommendations, on a periodic basis for the purposes of homeland secu rity, including the enhancement of domestic pre- paredness for and collective response to a cyber a tack by a terrorist, nation-state, or other pers and for other purposes.

''(2) ELEMENTS OF THE REPORT.—The Secretary shall—

''(A) include in the reports under this section findings regarding a cyber vulnerability or terrorist threat or potential terrorist threat, a nation-state threat or potential threat to critical electric infrastructure; and

''(B) provide recommendations regarding actions that may be performed to enhance individualized and collective domestic preparedness and response to the cyber vulnerability or terrorist or nation-state.

''(3) TRANSMITTAL OF REPORT.—The Secretary of Homeland Security shall transmit reports prepared in response to the cyber vulnerability or threat to the Commission and the appropriate committees of Congress, including the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate, of the Secretary's determinations under this section. Each such report may contain a classified annex.

''(4) TIMELY DETERMINATION.—If, in carrying out the assessment required under paragraph (1), the Secretary of Homeland Security determines that a significant cyber vulnerability or threat to critical electric infrastructure has been identified, the S

retary of Homeland Security shall communicate such a determination to the Commission in a timely manner. The Secretary of Homeland Security may incorporate intelligence or information received from other national security or intelligence agencies making such determination.

''(c) COMMISSION AUTHORITY.—

''(1) ISSUANCE OF RULES OR ORDERS.—Following receipt of a finding under subsection (b), Commission shall issue (and from time to time thereafter amend) such rules or orders as are necessary to protect critical electric infrastructure against vulnerabilities or threats.

''(2) EMERGENCY PROCEDURES.—The Commission may issue, in consultation with the Secretary Homeland Security, a rule or order under this section without prior notice or hearing if it determines the rule or order must be issued immediately to protect critical electric infrastructure from an imminent threat or vulnerability.

''(d) DURATION OF EMERGENCY RULES OR ORDERS.—Any rule or order issued by the Commission without prior notice or hearing under subsection (c)(2) shall remain effective for not more than 90 days unless, during such 90 days, the Commission gives interested persons

opportunity to submit written data, views, or argumen
(with or without opportunity for oral presentation) and
firms, amends, or repeals the rule or order.

''(e) JURISDICTION.—Notwithstanding section 201,
the provisions of this section shall apply to any enti
owns, controls, or operates critical electric infrastr
and such entities shall be subject to the jurisdiction
Commission for purposes of carrying out this section a
for purposes of applying the enforcement authorities
this Act with respect to such provisions, but shall
make an electric utility or any other entity subject t
jurisdiction of the Commission for any other purposes.

''(f) PROTECTION OF CRITICAL ELECTRIC INFRA-
STRUCTURE INFORMATION.—The provisions of section
214 of the Homeland Security Act of 2002 (6 U.S.C. 133)
shall apply to critical electric infrastructure infor
submitted to the Commission under this section to th
same extent that they apply to critical infrastructur
formation voluntarily submitted to the Department of
Homeland Security under that Act (6 U.S.C. 101 and fol
lowing).

“SEC. 224B. PROTECTION AGAINST KNOWN CYBER VULNERABILITIES OR THREATS TO THE CRITICAL ELECTRIC INFRASTRUCTURE.

‘‘(a) INTERIM MEASURES.—After notice and opportunity for comment, the Commission shall establish, consultation with the Secretary of Homeland Security, rule or order, within 120 days of enactment of this sec such mandatory interim measures as are necessary to pro tect against known cyber vulnerabilities or threats to reliable operation of the critical electric infrastruc the United States. Such interim reliability measures:

‘‘(1) shall serve to supplement, replace, or mo ify cybersecurity reliability standards that, as o date of enactment of this section, were in effect suant to section 215, but that are determined by t Commission, in consultation with the Secretary of Homeland Security and other national security agencies, to be inadequate to address known cyber vulnerabilities or threats; and

‘‘(2) may be replaced by new cybersecurity reli ability standards that are developed and approved pursuant to section 215 following the date of enac ment of this section.

‘‘(b) PLANS.—The rule or order issued under this subsection may require any owner, user or operator of c ical electric infrastructure in the United States to d

a plan to address cyber vulnerabilities or threats iden by the Commission and to submit such plan to the Com- mission for approval.''.

SEC. 2. EVALUATION OF EXISTING AUTHORITIES.

Section 214 of title II, subtitle B of the Homela Security Act of 2002 (6 U.S.C. 133(i)) is amended by ad ing at the end the following:

''(i) REVIEW OF AUTHORITIES TO PROTECT CRIT- ICAL INFRASTRUCTURE.—The Secretary of Homeland Se- curity shall evaluate the capacity and authority of th partment of Homeland Security and other Federal agen- cies to ensure the security and resilience of electron vices and communication networks essential to each of t critical infrastructure sectors identified pursuant Homeland Security Presidential Directive 7 against a cyber attack by a terrorist, nation-state, or other pe for the purpose of enhancing domestic preparedness fo and collective response to, a cyber attack by a terro nation-state, or other person and to enhance the Natio homeland security posture.''.

fi